REMARKS/ARGUMENTS

Applicant would like to thank the Examiner for the careful consideration given the present application. The application has been carefully reviewed in light of the Office action, and amended as necessary to more clearly and particularly describe the subject matter that applicant regards as the invention.

Claims 1-13 have been canceled. New claims 14-25 have been added. Six independent claims (1, 7, 8, 11, 12 and 13) have been canceled and six independent claims added (14, 15, 18, 21, 22 and 25). No extra claim fees are incurred by the present amendment.

Claims 1, 7, 8 and 11 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite. Claims 1, 7, 8 and 11 have been canceled.

Claims 1, 2 and 5-11 were rejected under 35 U.S.C. 103(a) as being unpatentable over DeTreville in view of Barlow. Claims 3 and 4 were rejected under 35 U.S.C. 103(a) as being unpatentable over DeTreville in view of Barlow and further in view of Gould. Claim 12 and 13 were rejected under 35 U.S.C. 103(a) as being unpatentable over DeTreville in view of Lee. As noted above, claims 1-13 have been canceled.

Discussion of New Claims 14 and 22

New claim 14 has been added by the present amendment. In the subject matter of claim 14, a secure device for holding data authenticates the validity of an application running unit. The application running unit, which is successful in this authentication, calculates digest data of an application. The application running unit sends the digest data to the secure device after the validity of the application running unit is authenticated by the secure device. The secure device carries out authentication of the application using the digest data.

The secure device itself does not generate the digest data of the application using data held by the secure device. Alternatively, the application running unit, whose validity was authenticated by the secure device itself, generates the digest data. Accordingly, it is not necessary for the secure device to have a function for calculating the digest data, and it is possible to simplify the configuration of the secure device. In addition, by having the application running unit, whose validity is authenticated by the secure device itself, calculate the digest data used for authentication of the application, it is possible to concatenate the validity judged by the secure device itself up to the digest data used by the secure device for judgment of validity of the application. So, by carrying out authentication using this digest data, an authenticated result is obtained, which is reliable with a nearly equivalent level to the case in which the secure device itself generates the digest data.

New claim 22 has also been added by the present amendment. In the subject matter of claim 22, the secure device manages data used by the application. In order to prevent this data from being utilized in an unauthorized manner, it is insufficient that the secure device merely authenticates the application. This is because the application is normally operating on other software, such as a BIOS and an OS. When the BIOS and OS are falsified into unauthorized ones, even if the application is an authorized one, there is no guarantee that data handed over to that application will be treated appropriately. However, should the secure device undertake the authentication of all constituent elements that configure the system (e.g., authenticate the BIOS, OS, application executing software, etc.), a heavy load is applied to the secure device.

In the subject matter of claim 22, authentication processing performed by the secure device can be limited to only authentication of the BIOS that operates first in the system, or to the authentication of the BIOS and some part of the authentication processing of an application.

Thereby, the secure device's authentication processing load is reduced considerably. In addition, about each configuration of OS, executing software etc. whose authentication is not carried out by the secure device itself, the authentication is entrusted to BIOS authenticated by the secure device, and OS authenticated by the BIOS. Accordingly, the authentication is carried out indirectly. In the subject matter of claim 22, the secure device has authenticated the BIOS. Therefore, a constituent element authenticated by the BIOS, and another constituent element further authenticated by the constituent element which was authenticated by the BIOS, are also reliable to the secure device. In the subject matter described in the claim 22, the secure device itself need not carry out authentication of constituent elements, such as the OS etc., but it is possible to obtain an authenticated result that is reliable with a nearly equivalent level to the case in which the secure device carried out authentication of all configurations from BIOS up to an application. Then, after this authentication is fully completed, access to data by the application is allowed, and thereby, it is possible to prevent data from being utilized in an unauthorized system.

Discussion of Cited References

DeTreville (USPN 6,609,199)

The cited document DeTreville is an invention relating to a smart card, and a device in which an application using data recorded on the smart card is operated. In the cited document DeTreville, a smart card, which received a request of data from an application, returns a certificate request to a device. The device, which received the request, returns a Certificate Chain indicating validity of OS and the application. Here, the Certificate Chain is information including a boot log etc. of the device (column 9, lines 5 - 12, column 24, etc.). The smart card

confirms the certificate and thereby, confirms whether the OS and the application, which a user itself desires, are operating or not, and then, allows the application to utilize the data.

However, the cited document DeTreville does not disclose that an application running unit of a terminal device calculates digest data of the application and sends the digest data to a verifying unit of a secure device after the validity of the application running unit is verified by the verifying unit, as described in the amended claim 14. In the cited document DeTreville, the smart card (which corresponds to the secure device in the present application) confirms validity of the entire device by use of the Certificate Chain including a boot log of the device, and therefore, there is no teaching that a constituent element, which was authenticated by the secure device, generates digest data of still another constituent element, after the authentication. Therefore, DeTreville has no disclosure or suggestion of a characteristic concept of new claim 14, specifically that the generation of digest data is entrusted to an application running unit that is verified by the secure device itself. Corresponding limitations are found in new independent claims 15, 18 and 21.

Further, DeTreville does not disclose that a secure device for managing data used by an application verifies validity of a BIOS, and the BIOS verifies validity of an OS after the verification by the secure device, and the OS verifies validity of executing software (that executes the application) after the verification by the BIOS, and the executing software performs at least a part of processing of verifying validity of the application after the verification by the OS, and the secure device allows the application to use the data after the validity of the application is verified, as described in new claim 22. In the cited document DeTreville, the smart card (which corresponds to the secure device in the present application) confirms validity of the entire device by use of Certificate Chain including a boot log of the device. DeTreville

has no disclosure or suggestion of a characteristic concept of new claim 22, specifically that the secure device for managing data used by the application entrusts a first constituent element (e.g., BIOS) authenticated by the secure device, and entrusts another constituent element (e.g., OS) authenticated by the first constituent element, for verification of OS, executing software, etc. which becomes a base on which the application is executed. Corresponding limitations are found in new independent claims 25.

Barlow (USPN 6,484,259)

The cited document Barlow is an invention relating to an authentication system using a portable token. Barlow is characterized by providing API for intermediating exchanges of cipher processing between a device and a token, in order to enable associating with various tokens, even if a device in which a token is inserted is a static one. In addition, it discloses that a functional section for carrying out cipher processing is disposed in the device fixedly (column 8, etc.).

However, the Barlow does not disclose that an application running unit of a terminal calculates digest data of the application and sends the digest data to the verifying unit (of a secure device) after the validity of the application running unit is authenticated by the verifying unit, as described in new claim 14. Therefore, Barlow does not teach or suggest a characteristic concept of claim 14, which is that the generation of digest data is entrusted to the application running unit that is verified by the secure device itself.

Further, Barlow does not disclose that a secure device for managing data used by an application verifies validity of a BIOS, and the BIOS verifies validity of the OS after the verification by the secure device, and the OS verifies validity of the executing software after the verification by the BIOS, and the executing software performs at least a part of processing of

verifying validity of the application after the verification by the OS, and the secure device allows the application to use the data after the validity of the application is verified, as described in new claim 22. Barlow has no disclosure or suggestion of a characteristic concept of new claim 22, specifically that the secure device for managing data used by the application entrusts a first constituent element (e.g., BIOS) authenticated by the secure device, and entrusts another constituent element (e.g., OS) authenticated by the first constituent element, for verification of OS, executing software, etc. which becomes a base on which the application is executed.

Lee (USPN 7,000,249)

The cited document Lee discloses a technique of authenticating a BIOS by use of information of a card possessed by a user at the time of booting up the BIOS, and booting up BIOS if the authentication is successful. However, Lee does not disclose that an application running unit of a terminal calculates digest data of the application and sends the digest data to a verifying unit (of a secure device) after the validity of the running unit is authenticated by the verifying unit, as described in new claim 14. Therefore, Lee does not teach or suggest a characteristic concept of new claim 14, which is that the generation of digest data is entrusted to the application running unit that is verified by the secure device itself.

Further, Lee does not disclose that a secure device for managing data used by an application verifies validity of a BIOS, and the BIOS verifies validity of the OS after the verification by the secure device, and the OS verifies validity of the executing software after the verification by the BIOS, and the executing software performs at least a part of processing of verifying validity of the application after the verification by the OS, and the secure device allows the application to use the data after the validity of the application is verified, as described in new

claim 22. Lee has no disclosure or suggestion of a characteristic concept of new claim 22, specifically that the secure device for managing data used by the application entrusts a first constituent element (e.g., BIOS) authenticated by the secure device, and entrusts another constituent element (e.g., OS) authenticated by the first constituent element, for verification of OS, executing software, etc. which becomes a base on which the application is executed.

Combination of Cited References

As described above, none of the cited documents DeTreville, Barlow and Lee teaches or suggests an application running unit of a terminal calculates digest data of the application and sends the digest data to the verifying unit (of a secure device) after the validity of the application running unit is authenticated by the verifying unit, as described in new claim 14. Therefore, even if these cited documents are combined, the claimed subject matter cannot be obtained.

In addition, as described above, none of the cited documents DeTreville, Barlow and Lee teaches or suggests that a secure device for managing data used by an application verifies validity of a BIOS, and the BIOS verifies validity of the OS after the verification by the secure device, and the OS verifies validity of the executing software after the verification by the BIOS, and the executing software performs at least a part of processing of verifying validity of the application after the verification by the OS, and the secure device allows the application to use the data after the validity of the application is verified, as described in new claim 22. Therefore, even if these cited documents are combined, the claimed subject matter cannot be obtained.

In view of the differences between the subject matter of new claims 14-25 and the cited references, applicant respectfully submits that said claims are allowable over the cited references.

In light of the foregoing, it is respectfully submitted that the present application is in condition for allowance and notice to that effect is hereby requested. If it is determined that the application is not in condition for allowance, the Examiner is invited to initiate a telephone interview with the undersigned attorney to expedite prosecution of the present application.

If there are any additional fees resulting from this communication, please charge same to our Deposit Account No. 16-0820, our Order No. NGB-36483.

Respectfully submitted,
PEARNE & GORDON, LLP

By: Brad C Spencer
Brad C. Spencer, Reg. No. 57076

1801 East 9th Street
Suite 1200
Cleveland, Ohio 44114-3108
(216) 579-1700

Date: November 10, 2008